Natural Security

The following enhancements will be provided with Natural Security Version 4.1:

- Logon Procedure
- Administrator Services
- Two-Phase Maintenance and Activation of Security Profiles
- Library Profiles
- Utility Profiles
- Links
- Functional Security
- Batch Mode
- Transferring Security Data
- Interface Subprograms

The following enhancements will be provided:

- It will be possible to define a warning message "your password will expire in *nnn* day" which will be issued to users at the initial logon. In addition, you will be able to set an activation date for this message.
- The number of unsuccessful logon attempts will be passed as a parameter to the logon-related user exit LOGONEX1. Thus, it will be possible, for example, to display corresponding information to the user *before* the maximum number of logon attempts is reached.

Administrator Services

Default Profiles

At present, default security profiles can only be defined for users. With Version 4.1, it will also be possible to define default profiles for all other types of Natural Security objects.

Two-Phase Maintenance and Activation of Security Profiles

At present, when a security profile is created or modified, its definitions are "activated" - that is, take effect - immediately (unless an activation date is set, of course); that is, the maintenance work of specifying definitions and the "activation" of these definitions are done simultaneously and lie in the hands of the same person.

With Version 4.1, a new two-phase mechanism will be provided which will allow you to separate maintenance from activation: one user will be allowed to do the actual maintenance work, that is, enter or modify the data in a security profile; however, these specifications/changes will only take effect after another administrator has authorized them. Unlike countersignatures, this authorization will not be given prior to an individual maintenance task to be performed, but at any time after the maintenance task, and it can be given for multiple security profiles all in one go. This will allow you to distribute the workload involved in maintaining security profiles without undermining the protection and control mechanisms provided by Natural Security’s administrator concept.

Library Profiles

Statement and Command Restrictions

The use of the new statements and system commands provided with Natural Version 4.1 can also be controlled with Natural Security.

Private Libraries

At present, access to a private library is restricted to the user for whom the private library is defined.

With Version 4.1, it will be possible to remove this restriction: Private libraries will then be treated like other "normal" library, and you will be able to control their use like that of other libraries.

This will be implemented as follows:

- A general option will be provided with which you can determine whether the old (Version 3) or new (Version 4.1) private library concept is to apply.
- If you select the old concept, the handling of private libraries will be unchanged, as it is now.
- If you select the new concept, you will be able make a type specification for each private library individually within its security profile:
  - Type A: The library can only be accessed by the user to which it is attached, that is, whose user ID is the same as the library ID (as with Version 3).
  - Type B: The library is treated like an unprotected library, that is, it may be accessed by any user.
  - Type C: The library is treated like a protected library, that is, it may only be accessed by the user whose ID is the same as the library ID and by users who are linked to it (or are in a group linked to it).
- Private libraries of type A will continue to be maintained in the the user maintenance section of Natural Security, whereas private libraries of types B and C will be maintained in the library maintenance section.
- An interface subprogram will be provided to facilitate the transition from the old to the new concept.

Linking Users to Libraries

At present, it is not possible to establish a link between a user and an unprotected library. The conditions of use of the library are determined by the library profile.

With Version 4.1, it will be possible to establish a special link between an administrator (or group of administrators) and an unprotected library. Thus it will be possible to define special conditions of use for administrators if this should be required for administration or maintenance tasks.

Copying Libraries

For the Copy Library function, a new option "with links" will be provided. This will allow you to copy not only the library profile, but also existing links associated with that library profile (similar to the "with links" option of the Copy User function).

Copying, Renaming and Deleting Libraries

At present, when you copy, delete or rename a library security profile on the FSEC system file, this has no effect on the library itself and its contents stored on the FUSER system file.

With Version 4.1, a new option will allow you to also adjust the FUSER system file accordingly when a library profile is copied, deleted or renamed: the contents of the library on the FUSER file would then also be copied to another library, deleted, or moved to another library.

Utility Profiles

With Version 4.1, it will be possible to control the use of the Natural utilities SYSTP and SYSDB2.

Links

At present, when you invoke a function for the maintenance of links, you will get a list of all objects to which the selected object can be linked, that is, those for which links already exist and those for which not.

With Version 4.1, an new option will be provided which allows you to display either a list of all linkable objects or a list of only those objects which are already linked. This new option will be available for all link maintenance functions.

Functional Security

If the status of a command processor is "modified" or "unresolved" (that is, modified or deleted with SYSNCP), you have to update or delete respectively the functional security defined in Natural Securitry for the command processor. At present, you have to make this adjustment for each command processor individually. With Version 4.1, an new option will allow you to automatically update/delete the functional security of all "modified" or "unresolved" command processors.

Batch Mode

At present, mailboxes are not displayed in batch mode. With Version 4.1, it will be possible to define for each mailbox whether it is to be output in batch mode or not. In addition, it will be possible to set in Administrator Services a general option which determines whether mailboxes are to be output in batch mode or not.

Transferring Security Data

New import and export functions will be provided for the transfer of security data between FSEC system files. These new functions will replace the existing programs SECULD and SECLOAD and will provide for enhanced and expanded transfer capabilities. The new functions will not only be available as menu-driven functions (like SECULD and SECLOAD), but also via direct commands to be applied to individual security profiles: you will, for example, be able to unload/load a single security profile by marking it with the corresponding command on a profile maintenance selection list.

SECULD and SECLOAD will cease to be supported with one of the subsequent releases.

Interface Subprograms

- New interface subprograms will be provided to perform mailbox maintenance functions from outside the Natural Security library SYSSEC.
- A new interface subprogram will allow you to retrieve the user name belonging to a specific user ID, and the user ID belonging to a specific user name.

